REMARKS

A. The Objections to Claims 1, 3-5, 7, 8 and 25-29

Claims 1, 3-5, 7, 8 and 25-29 were objected to based on an informality. In response, the Applicants have amended these claims to remove the informality. These amendments are not related to the patentability of these, or any other, claims. Accordingly, these objections now appear to be moot.

Applicants add these additional comments. In a previous Office Action the Examiner objected to the Applicants' use of the phrase "operable to". Though the Applicants believe this phrase is completely acceptable, to expedite examination the Applicants revised the claims. However, rather than expedite examination the opposite occurred; the Examiner objected to the revised claims.

In the next Office Action the Applicants request that the Examiner either withdraw the objections completely or indicate acceptable terminology. Absent one or the other the Applicants reserve their right to argue that the present phrase, as well as all previous phrases, are acceptable on appeal.

B. The Section 103 Rejections Based on Kanakubo

Claims 1, 3-5, 7-9, 11-13, 15-17, 19-21 and 23-29 were rejected under 35 U.S.C.§103(a) based on the combination of U.S. Patent Publication Application No. 20030147346 to Kanakubo (Kanakubo) and U.S. Patent Publication Application No. 20040004937 to Skalecki (Skalecki). Applicants disagree and traverse these rejections for at least the following reasons.

(i) claims 1, 3, 4, 9, 11, 12, 17, 19, 20 and 25-29

Each of independent claims 1, 9, 17, 25 and 28 (and their dependent claims) include the features of: (a) detecting a failure along an ingress region of a primary path; and (b) re-routing traffic from the primary path associated with an original Internet Protocol (IP) address to an alternate path….while associating the original IP address to the alternate path upon detection of the failure. Kanakubo does not disclose or suggest such features.

First, Applicants note that it is very difficult to understand the Examiner's rationales regarding Kanakubo. This might be because the disclosure in Kanakubo is itself ambiguous. Interpreting Kanakubo as best as possible, it does not appear that Kanakubo discloses the claimed inventions.

(a) Kanakubo Does Not Disclose The Claimed Ingress Region, Fault Detection

Kanakubo repeatedly refers to "remote fault" detection (*see, for example,* paragraphs [0015]) and ([0034]).

Kanakubo also states that, "[i]n the case where a fault occurrence 'a1' of label switched path is detected in the label switching router (LSP-F) 3 other than the label switching router (LSP-P) 1" a "fault indication retrieval table" is retrieved (*see* paragraph [0027]). In other words, Kanakubo appears to be directed to faults other than those involving a source router (LSP-P is a source router).

Taken together, the most reasonable interpretation of these statements is that Kanakubo is not directed at the detection of a fault along an ingress portion of a primary path as in claims 1, 9, and 17 or the detection of a fault along an ingress section of a primary path that comprises a link associated with a source network device, as in claims 25 and 28 (and their dependent claims). Instead, it is directed at the detection of faults that occur at locations that are remote from an ingress region or source router.

The Examiner's position, "that the 'ingress region' can be anywhere in the network as long as the region is input/incoming region/area/paths of the network" (see page 3 of the Final Office Action) is impermissible. Further, regardless of the Examiner's interpretation, the Examiner appears to ignore the teachings in Kanakubo that teach away from ingress region, fault detection.

As the Examiner knows well, though claims may be interpreted broadly any interpretation must be reasonable in light of the specification, *In re Hyatt,* 54 USPQ 2d 1664, 1667 (Fed.Cir. 2000). The specification provides two examples of an "ingress region". The first is "along an outgoing link associated with a source network device" (paragraph [0004]). The second is "at a network device which neighbors the source network device, a so-called neighboring device" (paragraph [0004]).

Thus, the Examiner's interpretation of the phrase "ingress region" is impermissible because it is not reasonable in light of the teachings of the specification.

Further, to the extent Kanakubo's disclosure can be understood, the fault shown in Fig.1 is not along an outgoing link associated with a source network device (e.g., LSR-P 1) or at a

network device (e.g., LSR 2) which neighbors the source network device. This fact coupled with Kanakubo's apparent focus on remote fault detection leads to the conclusion that Kanakubo does not disclose the ingress region, fault detection features set forth in claims 1, 9, 17, 25 and 28 (and their dependent claims).

(b) Kanakubo Does Not Disclose the Association of a Primary Path's, Original IP Address to an Alternate Path

Claims 1, 9, 17, 25 and 28 (and their dependent claims) also include the feature of re-routing traffic from a primary path associated with an original Internet Protocol (IP) address to an alternate path while associating the original IP address to the alternate path upon detection of the failure. In contrast, Kanakubo appears to suggest the opposite; namely, that the address of a primary path is replaced with a different address when an alternative path is used.

The Examiner repeatedly refers the Applicants to Fig. 3 of Kanakubo which depicts a "LSP Fault Indication Retrieval Table" ("Table"). To the extent that the description of this Table can be understood, it does not appear that the Table includes a value that indicates an original IP address of a primary path is associated with an alternative path.

Paragraphs [0039] through [0045] describe the contents of Kanakubo's Table. More particularly: the column in the Table labeled "Indicated Protection Point" appears to identify the IP address of a router that will be used as a "protection point" (e.g., address of the first router in an alternative path, *see* paragraphs [0040] and [0042] through [0045]) or the address of a router that will "stop the [differentiated] service" (*see* paragraph [0041]); the column labeled "Entry Type" describes the type of path (*see* paragraphs [0040] and [0042] through [0045]); and the column labeled "Entry" identifies the routers that are to be bypassed (*see* paragraphs [0040] and [0042] through [0045]). There does not appear to be any entry in Kanakubo's Table that indicates that an original IP address of a primary path becomes associated with an alternative path.

In fact, Kanakubo appears to be mostly silent as to the details of its address association (i.e., in Kanakubo terminology, how packets are switched from one path to another). For example, Kanakubo states that after a "fault indication packet is received…..the switching of the

corresponding label switched path is performed (step S8 in Fig. 6)" (*see* paragraph [0053]). However, thereafter, no details of the switching process appear to be described.

Further, to the extent Kanakubo does discuss its switching process, it appears to imply that, switching from a primary path to a secondary path "may involve replacement of the label value" (*see* paragraph [0055]). Said another way, rather than use the original address of a primary path as the address of an alternative path the original address is replaced with a different address.

(ii) claims 5, 7, 8, 13, 15, 16, 21, 23 and 24

(a) Kanakubo Does Not Disclose Maintaining The Same QoS

Each of independent claims 5, 13 and 21 (and their dependent claims) include the feature of re-routing traffic from a primary path associated with an original IP address to an alternate path, wherein the alternate path comprises devices that maintain the same quality of service as the primary path.

The only, apparently relevant discussion of quality of service (QoS) in Kanakubo appears in paragraphs [0041] and [0060]. Paragraph [0041] implies that an LSP-P router will "stop" a differentiated service while paragraph [0060], in pertinent part, states: "In this example, the label switched path is designated in the entry within the message of the LSP fault indication. However, it is possible to designate not only the label switched path but also the operation policy (e.g., QoS policy)". Though it is difficult to tell what "example" is being referred to in paragraph [0060], it appears to be the "fast switching" of multiple, label switched paths discussed in paragraph [0059]. The excerpt in paragraph [0060] is silent with respect to whether the original address of a primary path is maintained as the address of an alternative path. No mention of a primary or alternative path is made, nor maintenance of an original address. For the most part, this excerpt implies that the QoS of some LSP is included in a fault detection message. What address, and how the address is used, is not described.

Further, any implication that the QoS of a primary path is maintained in an alternative path appears to be rebutted by Kanakubo's statement in paragraph [0041] that an LSP-P router "stops" differentiated services.

(b) Kanakubo Does Not Disclose Maintenance of a Primary Path's, Original IP Address

Independent claims 5, 13 and 21 (and their dependent claims) also include the feature of re-routing traffic from a primary path associated with an original IP address to an alternate path while maintaining the original address. As discussed above with respect to claims 1, 3, 4, 9, 11, 12, 17, 19, 20 and 25-29, Kanakubo appears to suggest the opposite: that the address of a primary path is not maintained. Instead, it is replaced with a different address when an alternative path is used.

(iii) Skalecki

Skalecki does not make up for the deficiencies of Kanakubo.

Accordingly, Applicants respectively request withdrawal of the rejections and allowance of claims 1, 3-5, 7-9, 11-13, 15-17, 19-21 and 23-29.

C. The Section 103 Rejections Based On Dantu

Claims 1, 3-5, 7-9, 11-13, 15-17, 19-21 and 23-29 were rejected under 35 U.S.C.§103(a) based on the combination of U.S. Patent No. 7,167,443 to Dantu (Dantu) and Skalecki. Further, the same claims were rejected based on a combination of Dantu and U.S. Patent No. 5,838,924 to Anderson ("Anderson"). Applicants disagree and traverse these rejections for at least the following reasons.

(i) Dantu Does Not Disclose the Alternative Paths as in Claims 5, 7, 8, 13, 15, 16, 21, 23 and 24

Independent claims 5, 13 and 21 (and their dependent claims) include the feature of re-routing traffic from a primary path associated with an original IP address to an alternate path while maintaining the original address, where the alternate path comprising devices which *are not a part of the primary path except for a network device that has received a failure message and a destination network device*. Dantu does not disclose or suggest such a feature.

Instead, in Dantu, upon detection of a "link failure" packets are transmitted through a "protection path" which includes nodes that are also a part of an original "working path", where the nodes are other than the network device that has received a failure message and destination network device.

(ii) Dantu Does Not Disclose the Association of a Primary Path's, Original IP Address to an Alternate Path or the Maintenance of such an IP Address as in Claims 1, 3-5, 7-9, 11-13,15-17, 19-21 and 23-29

Independent claims 1, 5, 9, 13, 17, 21, 25 and 28 (and their dependent claims) include the feature of re-routing traffic from a primary path associated with an original Internet Protocol (IP) address to an alternate path while associating the original IP address to the alternate path or re-routing traffic from a primary path associated with an original IP address to an alternate path, where the rerouting maintains the original address. Dantu does not disclose or suggest either feature.

Dantu's discussion of fault detection and the use of protection paths occurs mainly in column 9, line 42 to column 12, line 38 and column 17, line 12 to column 20, line 30. Nowhere in this discussion does it appear that Dantu states, explicitly or implicitly, that the original address of a primary path becomes associated with, or is maintained by, an alternative path. To the contrary, Dantu appears to imply that addresses are changed. For example, Dantu states that "After the identifying step 1004, the ingress node 300 determines appropriate protection path label values for the affected data packets and sets the labels into the header of the outgoing data packets (step 1008). Finally, the affected data packets are generated onto the fiber optic ring network and are forwarded along the protection paths according to the *newly set* label values" (italics added).

(iii) Skalecki and Anderson

Neither Skalecki nor Anderson make up for the deficiencies of Dantu.

Accordingly, Applicants respectively request withdrawal of the rejections and allowance of claims 1, 3-5, 7-9, 11-13, 15-17, 19-21 and 23-29.

D. Entry of Amendment After Final

Entry of this Amendment After Final (AAF) is solicited because the AAF: (a) places the application in condition for allowance for the reasons discussed herein; (b) does not raise any new issues requiring further search and/or consideration; (c) does not present any additional claims without canceling the corresponding number of finally rejected claims (the claim amendments were direct at form, not substance); and (d) places the application in better form for appeal, if an appeal is necessary.

The Commissioner is authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 50-3777 for any additional fees required under 37 CFR § 1.16 or under 37 CFR § 1.17; particularly, extension of time fees.

Respectfully submitted,

CAPITOL PATENT & TRADEMARK LAW FIRM, PLLC

By: /John E. Curtin/
John E. Curtin, Reg. No. 37,602
P.O. Box 1995
Vienna, Virginia 22183
(703) 266-3330